Addonics
TECHNOLOGIES

User Guide

Secure NAS R5

(SN535E1G)

www.addonics.com

Firmware v87a

Technical Support
If you need any assistance to get your unit functioning properly, please have your product information ready and contact Addonics Technical Support at:

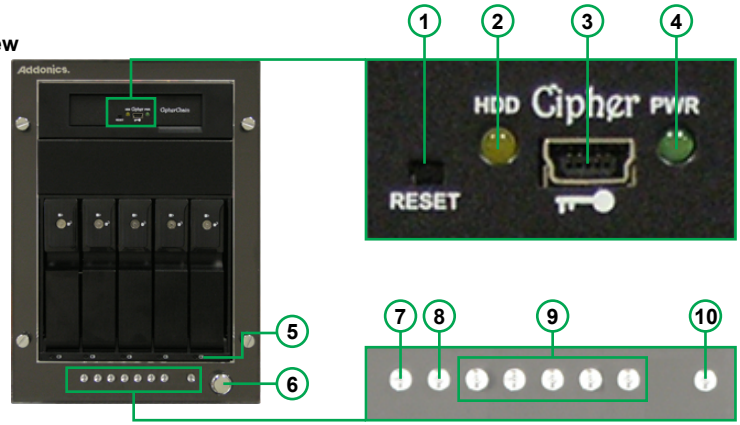
Hours: 8:30 am - 6:00 pm PST
Phone: 408-453-6212
Email: http://www.addonics.com/support/query/

Overview

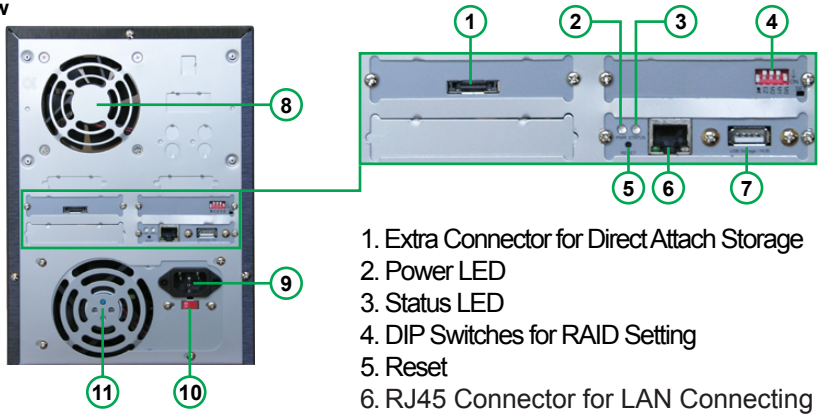
SN535E1G

1.Reset Button
2. HDD
3. Cipher Key Socket
4. Power
5. Drive Activity LED
6. Power
7. NAS Status
8. RAID Error
9. Drive Error
10. Power

Front View



Back View



1. Extra Connector for Direct Attach Storage
2. Power LED
3. Status LED
4. DIP Switches for RAID Setting
5. Reset
6. RJ45 Connector for LAN Connecting
7. USB Connector for Additional USB Storage
8. 40x40mm Cooling Fan
9. Power Cord Socket
10. 110 / 240 V Switch
11. 320w ATX Power Supply

Power Cord (U.S. Version Shown)

WARNING: Please remember to set the power supply to your local outlet voltage prior to plugging in the power cord. Failure to do so may damage the power supply.

eSATA Cable

Cipher Keys

Network Cable

Power LED (next to Power Switch): glows green while unit is turned on.
Power LED (on Cipher Chain Module): glows green when Cipher is unlocked.
Drive Activity LED: Glows blue to indicate power, flashes magenta (blue and red) to indicate activity.
HDD LED (on Cipher Chain Module): blinks to indicate RAID activity.
NAS Status LED (front and rear): glows when idle, blinks to indicate the unit is booting or busy.
RAID Error: glows to indicate the RAID is either degraded or offline, blinks to indicate rebuilding is in progress.
Drive Error: blinks to indicate a spare drive that is rebuilding.
RESET button (on Cipher Chain Module): press to activate with inserted key (or deactivate if no key is inserted).
RESET button (rear, on NAS module): press and hold as described in Resetting the NAS Unit.
SET button (rear, next to dipswitch): press and hold during power-up to set or reset the RAID setting.
POWER LED (rear, on NAS module): indicates the NAS module is powered up.
RAID Setting Dipswitch: used with SET button to define or delete a RAID array.
DAS Connector: used for connecting the RAID array to an external computer.
RJ45 Connector: used for connecting to 10/100/1000 Mbit network.
USB Connector: used for attaching additional USB 2.0 storage to the NAS unit.

Installation

Network Connection

The Secure NAS unit is factory configured for dynamic IP addressing (DHCP client). Connect the unit to a network (router or switch) where DHCP is supported. Static IP may be assigned later after initial setup.

Storage

The Secure NAS unit does not support FIS switching for port multipliers, otherefore the installed drives must be configured as a RAID array. Externally, through the use of USB hubs, up to a total of 16 physical storage devices may be connected, counting the Secure NAS unit's RAID array. One SATA port multiplier in JBOD mode may be connected using USB; however, with more than one such port multiplier connected only one will function – others will not be recognized at all.

Each physical unit may be formatted with up to 4 individual partitions using a Master Boot Record (MBR), or up to 15 individual partitions using a GUID Partition Table (GPT). Supported file systems are: FAT32, ext2, ext3, ext4, XFS, and NTFS. The NAS 4.0 unit will by far provide the best performance when using the XFS file system on the Secure NAS unit's RAID array.

NOTE: Initializing a drive with MBR is limited to drives less than 2TB in capacity with up to 4 partitions total. For drives greater than 2TB in capacity or if more than 4 partitions are desired, the drive must be initialized using a GPT boot record.

Cipher key

The two cipher keys have an identical, unique encryption code. One of these keys should be kept in a safe and secure location and can be sent back to Addonics for duplicating additional keys. If you are down to the last key, be sure to make a back up of all the data stored inside your NAS unit prior to sending the last key to Addonics. Addonics is not responsible for keys lost in the mail or for retrieval of the data inside the encrypted hard drive.
IMPORTANT: There is no back door for the Cipher tower encrypted hard drives if the Cipher keys are lost or stolen.

The Secure NAS unit's RAID Array is directly connected to the CipherChain module internally. The Cipher Key must be inserted before powering up the unit in order to configure the RAID array. During normal operation, the RAID array may only be accessed while the CipherChain module is unlocked by either powering up the unit or pressing the CipherChain RESET button while the Cipher Key is inserted. The POWER LED on the CipherChain module indicates the CipherChain is unlocked. If the CipherChain POWER LED is not glowing, the RAID array cannot be configured or accessed.

Drive Installation

1. Be sure all doors are unlocked, use the provided keys to unlock if needed.
2. Gently pull the lever on the door to release it.
3. Insert the drive as shown on the label inside the door: The SATA connector toward the rear, with label side to the right. The drive should slide in easily, don't force it.
4. Close the door on the drive bay. It should also give little resistance, don't force it. It can help to slightly tug the lever while snapping the door shut to make it easier. As soon as the drive is in position it will power up.
5. The drives may be locked in place if desired.

Direct Attached Storage ("DAS") Connector

The Secure NAS unit's RAID array may be connected from the DAS connector directly to a computer using the eSATA cable provided. This connection can be useful for adding content directly to the RAID array.

NOTE: The DAS Connector is a hardware controlled switch, activated by inserting an eSATA cable into the eSATA port on the back of the Secure NAS unit. The Secure NAS unit's RAID array will instantly disconnect from the NAS controller inside the unit, even if there is nothing connected to the other end of the eSATA cable. DO NOT connect an eSATA cable to the DAS Connector except when using the RAID array with an external computer.

RAID Configuration

The Secure NAS unit does not support SATA Port Multipliers. Using the unit with more than one drive requires a RAID configuration.

Using identical drives for all settings other than LARGE is strongly recommended. Creating a LARGE array using drives that have different properties will use all space on all members, and performance will match that of the member in use during any particular I/O operation. Creating a RAID using drives that are not all the same size will result in all members using only as much space as the smallest member. Creating a RAID using drives that have different performance will degrade the overall performance of the array.

Any number of drives may be installed in the unit, the RAID Modes available are as follows:

Number of drives	RAID Mode
1	JBOD Mode only
2	RAID 0, 1, CLONE, LARGE
3	RAID 0, 3, 5, CLONE, LARGE
4	RAID 0, 10, 3, 5, CLONE, LARGE
5	RAID 0, 3, 5, CLONE, LARGE

NOTE: RAID 0 and LARGE modes are NOT recommended for use on the Secure NAS unit.

RAID Modes
The Secure NAS unit supports one drive in JBOD Mode, several types of RAID and some non-RAID drive sets. Each configuration has different properties and requirements, as follows:

JBOD Mode (Individual Drives)
Number of drives: 1
Unit capacity: N/A
Spares: no
Fault tolerance: none
JBOD mode may only be used with one drive installed in the Secure NAS unit.

RAID 0 (Stripe set)
Number of drives: at least 2
Unit capacity: size of each member times number of members.
Spares: no
Fault tolerance: none - if any member is lost all data is lost (see note).
RAID 0 “stripes” the file system across the array by placing “chunks” of data sequentially between drives in a specific order.
NOTE: Risk of data loss compared to a single drive multiplies by the number of members in a RAID 0.

RAID 1 or 10 (Mirror set, Stripe of mirror sets)
Number of drives: 2 (RAID 1) or 4 (RAID 10).
Unit capacity: size of one member (RAID 1) or size of two members (RAID 10).
Spares: yes – if EZ mode is not disabled and 3 (RAID 1) or 5 (RAID 10) drives are present, the array will be initialized with a spare.
Fault tolerance: RAID 1 can withstand the loss of one drive without losing data.
RAID 10 can withstand the loss of one drive from each mirror set without losing data.
RAID 1 works by duplicating the exact same data on two drives.
RAID 10 works by using two RAID 1 sets configured as members of a RAID 0. Disks 1 and 2 are mirrored, disks 3 and 4 are mirrored, and the two mirror sets are striped together.

RAID 3 (Stripe set with dedicated parity)
Number of drives: at least 3
Unit capacity: size of one member times number of members minus one.
Spares: yes
Fault tolerance: can withstand the loss of one drive without losing data.
RAID 3 works by striping data for individual I/O blocks across all members except one, which contains parity data for the stripe set computed internally by the Port Multiplier. In the event of failure, the missing information can be calculated using the parity information.

RAID 5 (Stripe set with striped parity)
Number of drives: at least 3
Unit capacity: size of one member times number of members minus one.
Spares: yes
Fault tolerance: can withstand the loss of one drive without losing data.
RAID 5 works by striping entire I/O blocks across all members of the set, with each member taking turns carrying parity data computed by the Port Multiplier. In the event of failure, the missing information can be calculated using the parity information.

CLONE (Mirror set)
Number of drives: at least 2
Unit capacity: size of one member.
Spares: yes
Fault tolerance: can withstand the loss of any number of drives without losing data as long as at least one complete member remains online. CLONE mode works the same way as RAID 1, by maintaining a complete copy of the entire set of data on each drive.

LARGE (Spanned set)
Number of drives: at least 2
Unit capacity: 100% of all drives together regardless of differences in size
Spares: no
Fault tolerance: cannot withstand the loss of any drives without losing data. However, some data may be recovered as long as the drive(s) carrying the file system data (boot record, directory, etc.) remain online. LARGE mode is neither a RAID nor is it a JBOD. It works by declaring the sum of all available space of the member drives as a single unit, without striping the data. As each member is filled, new data is stored on the next.

Notes about Spare Drives
To create an array with one or more spares, set or modify the RAID mode while the spares are not inserted in the RAID array. When EZ mode is enabled (SW1:2 OFF), individual drives connected when an array is present are considered spare. Spare drives must be equal to or larger in size than the smallest member. When any type of array is defined, individual units will be considered spare.

If EZ mode is disabled (SW1:2 ON), all individual drives not configured as array members will be offered to the host adapter as separate units. The Secure NAS unit does not the Port Multiplier's switching protocol, so this feature is not supported.

RAID 0 and LARGE arrays are not fault-tolerant and spare drives will not be useful. When a spare drive is present and a fault-tolerant RAID (1, 10, 3, 5, or CLONE) is defined, EZ mode will automatically rebuild any available spares into the array to replace a failed member. During this process, the spare drive's Error LED will flicker along with the RAID Error LED until rebuilding is complete.

Configuring the RAID Using Dipswitches

Resetting the RAID

NOTE: This procedure destroys all RAID data. It should not harm individual drives or their contents; however, creating backups of all data is strongly recommended before proceeding.

Be sure the port multiplier is connected to an active host before proceeding. The port multiplier will not complete the process if it has no host connection.

1. Power down the unit and set the dip switch to the desired RAID Mode.
2. While holding the SET button, turn the unit on. A long beep will sound from the Port Multiplier. The SET button may be released once the long beep starts. Shortly after releasing the SET button, the port multiplier should “chirp” to indicate the process is complete. If instead of a chirp the Port Multiplier sounds a series of short beeps, an error has occurred during the process.

Setting or Modifying the RAID Mode

NOTE: Setting or modifying the RAID mode destroys all data.

Be sure the port multiplier is connected to an active host before proceeding. The port multiplier will not complete the process if it has no host connection.

1. Follow the procedure for resetting the RAID Mode.
2. Power down the unit and set the dip switch to the desired RAID Mode.
3. While holding the SET button with a ballpoint pen, turn the unit on. A long beep will sound from the Port Multiplier. The SET button may be released once the long beep starts.

Shortly afterward, the port multiplier should “chirp” to indicate the process is complete. If instead of a chirp the Port Multiplier sounds a series of short beeps, an error has occurred during configuration of the array.

BZS Switch (SW1:1):

The BZS switch is used to silence the audible alarm buzzer. The OFF position permits the audible alarm, and the ON position silences the audible alarm. The BZS switch has immediate effect.

EZ Switch (SW1:2):

The EZ (spare) switch inhibits spares when ON. When in the OFF position, all individual drives (not defined as members of an array) are considered spare and are not offered to the operating system. Should a RAID become degraded, when the EZ switch is in the OFF position a spare drive will be used automatically to rebuild the RAID, if present. EZ mode is determined when the unit is powered up. Changing the switch will have no effect until the unit has been re-powered.

Warning: turning off the EZ switch to rebuild an array will consider any drives not declared array members to be eligible for rebuild as a spare. Rebuilding will destroy all existing data on that drive and the drive chosen is not predictable. Disconnect any individual drives with valuable data on them before enabling EZ Mode.

RAID Mode Switches M2, M1, M0 (SW1:3 – SW1-5)
The RAID Mode switches define what type of RAID will be initialized when the unit is powered up while the RAID Mode button is held down, as follows:

Dipswitch Position	**1 (BZS)[1]**	2 (EZ)	3 (M2)	4 (M1)	5 (M0)
JBOD (Individual Drives) *** FACTORY DEFAULT SETTING**	OFF	**OFF[2]**	OFF	OFF	OFF
RAID 0	OFF	**ON[3]**	ON	ON	ON
RAID 1 OR 10	OFF	OFF	ON	ON	OFF
RAID 3	OFF	OFF	ON	OFF	OFF
RAID 5	OFF	OFF	OFF	ON	OFF
CLONE	OFF	OFF	OFF	ON	ON
LARGE	OFF	ON	ON	OFF	ON

NOTES:
1. Audible Alarm is recommended at all times.
2. EZ mode has no effect when no array is defined.
3. Disabling EZ for RAID 0 and LARGE is strongly recommended.

The NAS Controller Unit Boot Process
Upon powering up the unit, the status LED will blink at first between bright and dim, then remain dark for a few moments, then begin to blink between bright and dark for a while and finally settle down to glowing steadily. Once this pattern is complete the unit is ready to communicate.

This process normally takes about a minute or less, but may take longer depending on the complexity of the configuration, storage and LAN connections. With the 240 possible file systems, booting may take several minutes or longer.

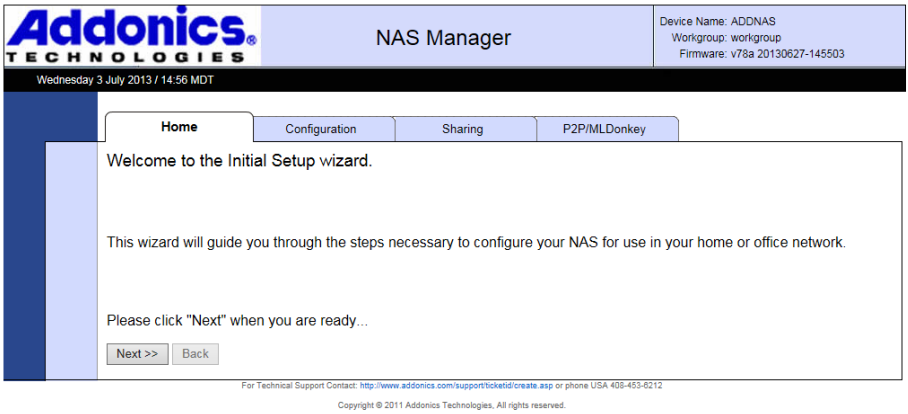
Resetting the NAS Controller
Should a problem arise with the NAS Controller or its configuration, the unit may be reset simply by turning the unit off, then back on after a few moments. If this doesn't clear the problem, the unit may be returned to its factory configuration by gently pressing and holding the reset button between the power and LAN connectors until the Status LED blinks slowly, then rapidly. After releasing the Reset button while blinking slowly there will be no changes. After releasing the button once the Status LED blinks rapidly, the Status LED will continue to blink for a while, and may possibly glow steadily for a while as well. Eventually it will begin the boot process, beginning with blinking between bright and dim. Once the boot process is complete and the LED is glowing steadily again, all settings will have been cleared and the unit is ready to communicate with all settings reset to the factory default – including the network and device name settings.
If the process appears to become stuck or takes too long to complete, you can try disconnecting power, then reconnect and after the Status LED blinks bright and dark a few times, try the Reset button again.

Initial Setup

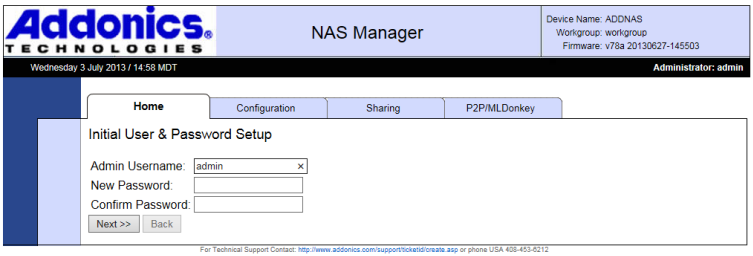
Windows: All of the Secure NAS unit's functions and features are configured using a Web Interface. Once the hardware is installed, access the Web Interface with a web browser on a computer attached to the same network by typing in “http://addnas” - this will work on most Windows systems. Be sure the computer accessing the NAS has the Workgroup name set to WORKGROUP.

MAC: Mac users may need to determine the Secure NAS unit's IP address by opening a Terminal window and typing the following command:
smbutil lookup addnas
This utility should return the Secure NAS unit's IP address. Typing this address into the web browser should open the Secure NAS unit's Web Interface.
Linux: Linux users may need to determine the Secure NAS unit's IP address if Windows name resolution support is not fully installed and configured, by examining the DHCP server's clients table and attempting to connect to each unidentified IP address using a browser until the Secure NAS unit's Web Interface appears.

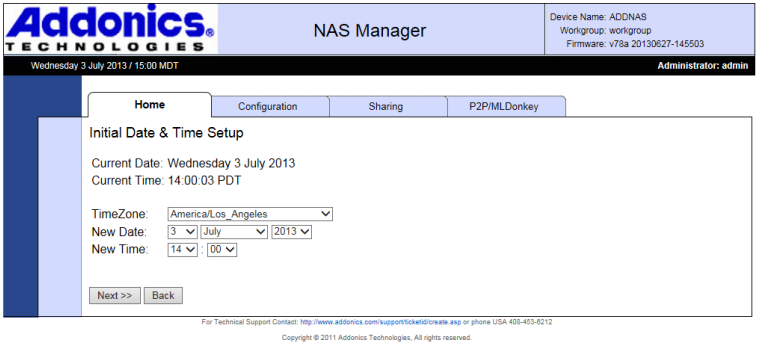
Once you have connected to the Web Interface, the Initial Setup page will appear:


Addonics TECHNOLOGIES
NAS Manager
Device Name: ADDNAS
Workgroup: workgroup
Firmware: v78a 20130627-145503
Wednesday 3 July 2013 / 14:56 MDT
Home
Configuration
Sharing
P2P/MLDonkey
Welcome to the Initial Setup wizard.
This wizard will guide you through the steps necessary to configure your NAS for use in your home or office network.
Please click "Next" when you are ready...
Next >>
Back
For Technical Support Contact: http://www.addonics.com/support/ticketid/create.asp or phone USA 408-453-8212
Copyright © 2011 Addonics Technologies, All rights reserved.

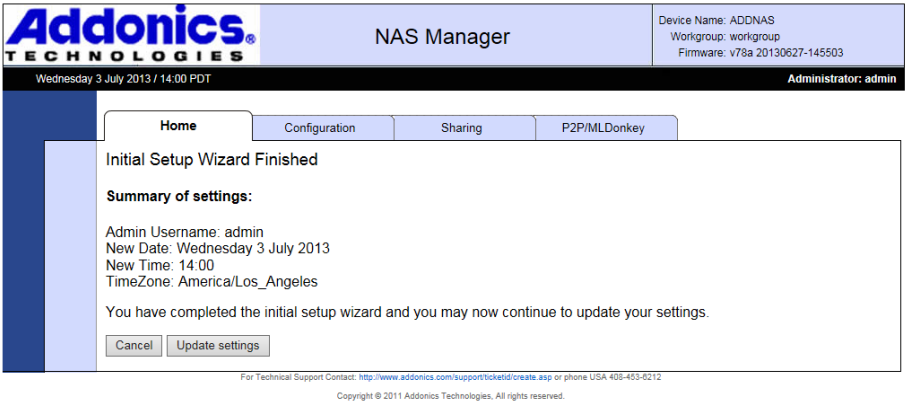
Click Next, then a dialog will appear requesting the Administrator login. The default username is "admin" and the password is "123456" (without the double-quote marks). Next, set a custom password for the admin account. The admin account name may also be changed.



Next, set up the Date and Time. Choose a city nearest you in the same Time Zone and be sure the Date and Time are correct.



Finally, review and confirm the settings:



After clicking on the Update settings button, Initial Setup is complete.

Sharing Files Using the Secure NAS

SMB (Windows Sharing)

Connecting to the NAS for direct file access through Windows Explorer is very similar to sharing files between Windows systems. Typing “\\ADDNAS” (or the Secure NAS unit's hostname if changed from the default) or the double-backslash followed by the Secure NAS unit's IP address is the easiest way to gain direct access quickly. After pressing Enter, the Explorer Window should show a list of the shares available. Opening any of the shares is like opening any other folder, except when accessing a share for the first time, Windows may request a username and password for access to the share (unless “Everyone” permissions have been changed from the default setting of NONE). Entering a valid username and password will open the folder with appropriate access rights to that user. If “NONE” permissions are set for that user on that share, Another username and password prompt will appear. After connecting to a share, Windows will use the same username and password for all connections until the Windows user logs off of Windows.

On Mac systems, on the Finder's Go menu choose “Connect to Server...” then in the server address box type “smb://” followed by the Secure NAS unit's IP address. On Linux systems, use the “Connect to share...” dialog found on the Nautilus or “File Manager” menu bar, then select Windows Share for the type and complete the remaining fields for share name, username and password. Information required to complete the connection and the system's response vary from one version of Linux to another, and should be expected to work about the same way as connecting to a share on an actual Windows PC.

FTP Server
The Secure NAS FTP Server requires the "User Home Directory Drive" is defined under the Sharing Tab to function. Anonymous login is supported with no user home directory and access to any shares with read-only or read and write access to "Everyone" for FTP. Authenticated users will have read and write access to their home folder and any other shares defined under the Sharing tab with read-only or read and write access for the user for FTP, as well as "Everyone."

Getting Started with MLDonkey

MLDonkey is a powerful, multi-protocol Peer-to-Peer (P2P) client included with the Secure NAS unit. The features and capabilities of this tool are beyond the scope of this user guide, the steps below will show how to get MLDonkey up and running. For more information on how to use MLDonkey, visit http://mldonkey.sourceforge.net.

MLDonkey Basic Setup
The MLDonkey client requires one partition formatted with either ext3 or XFS. The Secure NAS unit's format utility can format one physical unit with a single partition using all space if needed.

Under the P2P/MLDonkey tab, choose the drive you wish to create the file structure on and click Save. Please note: this menu will permit setting up folders on incompatible file systems. If this is done, MLDonkey will not start or may not be able to download files.

When the folder structure is set up, a page will appear stating this is done. Click the START button. NOTE: The MLDonkey setup page will create a share on the selected drive called MLDonkey. This share will be configured with “None” permissions to “Everyone” as well as all existing users.

Next, a new page will appear stating MLDonkey is running. Click the link at the bottom of the page that reads “Launch MLDonkey Control Panel.”

A new tab will appear in the browser with the MLDonkey web interface. If MLDonkey is not fully initialized yet, the browser may report a failure to connect. If this happens, wait about one minute and try again, either by refreshing the page or clicking a “try again” button – this step varies depending on the browser used.

When first setting up, a prompt appears warning there is no password for the admin account. Click the space between the “DL” and “Input” buttons, then type the command “useradd admin” as shown, then add a password after a space.

NOTE: The MLDonkey admin account is not the same account as the Secure NAS unit's web interface admin account. It is recommended that the password matches for simplicity, but not necessary.

MLDonkey will perform most of the remaining steps automatically and connect to some servers on the Donkey network.

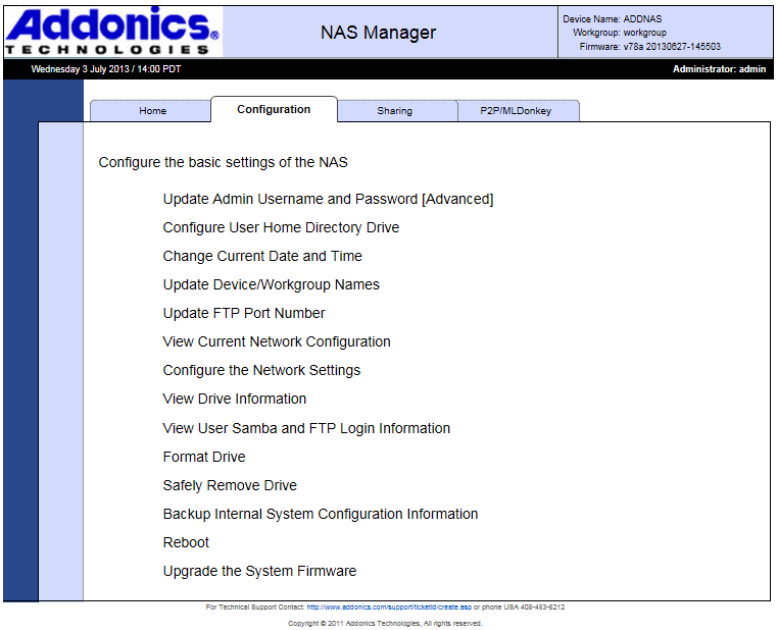
To download a file using the Donkey network, begin by clicking search, then enter some criteria and click the Search button. After a query message appears, click the "Search Results" button.

To download a Torrent, on the command bar type dllink followed by a space and the full URL path to the .Torrent file and press Enter or click Input. (example: "dllink http://sampletorrent.com/path/dot-torrentfile.torrent"). MLDonkey will parse the download and add it to the download queue automatically.

Files queued for download will appear in the MLDonkey share in the incoming/files folder when when complete.

NOTE: this folder has read-only permissions and cannot be changed.

The Configuration Tab



Update Admin Username and Password

Changes the web interface management login.

Configure User Home Directory Drive

Determines which drive on the system carries the HOME directory for users. The user's home folder is required for FTP transfers and as a network share for private files. If a home directory is already defined it will be shown. Choose a volume and click Save. If any files exist in a previous Home directory they will be moved to the new location.

Change Current Date and Time

Settings for time zone, date and time. Set time zone to a listed city nearby in the same time zone.

Update Device/Workgroup Names

Settings for the Secure NAS unit's network name and Windows workgroup. Default setting is ADDNAS joined to WORKGROUP. Setting the workgroup name on all devices on the same network to match is strongly recommended. The Device name is used for accessing the Web Interface as well as browsing for the shared folders on the network.

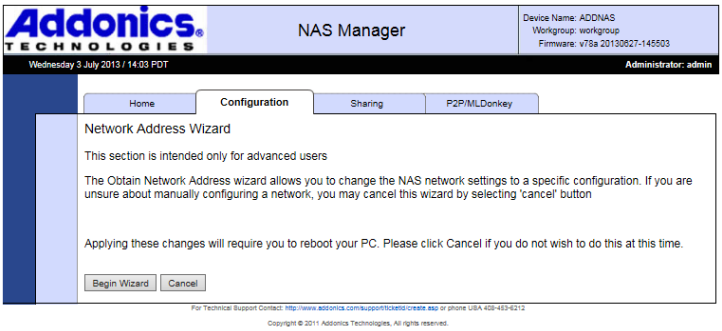
Update FTP Port Number

Changes the TCP Port used by the FTP server. Default is port 21. Note that some FTP clients will not be able to connect on alternate ports.

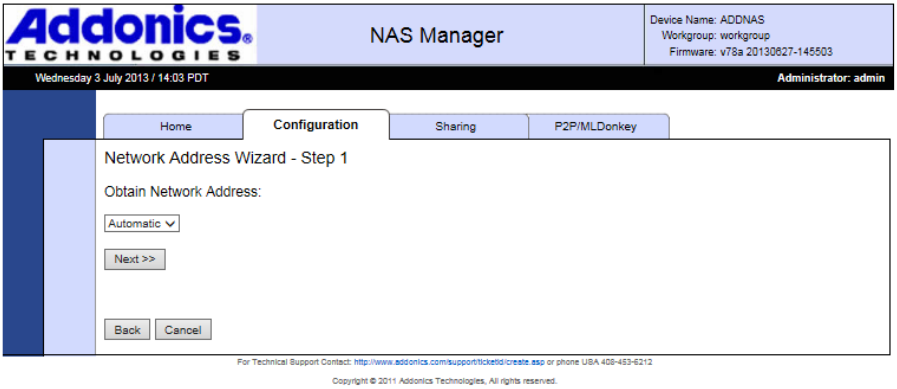
View Current Network Configuration
Displays details about the Secure NAS unit's current network settings. Includes device and network names as well as TCP/IP settings.

Configure the Network Settings

Starts the network configuration wizard.

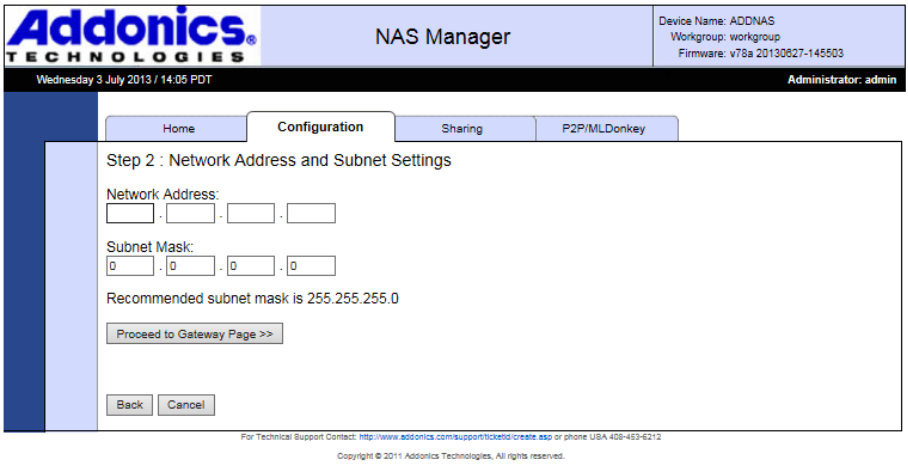

Addonics TECHNOLOGIES
NAS Manager
Device Name: ADDNAS
Workgroup: workgroup
Firmware: v78a 20130627-145503
Wednesday 3 July 2013 / 14:03 PDT
Administrator: admin
Home
Configuration
Sharing
P2P/MLDonkey
Network Address Wizard
This section is intended only for advanced users
The Obtain Network Address wizard allows you to change the NAS network settings to a specific configuration. If you are unsure about manually configuring a network, you may cancel this wizard by selecting 'cancel' button
Applying these changes will require you to reboot your PC. Please click Cancel if you do not wish to do this at this time.
Begin Wizard
Cancel
For Technical Support Contact: http://www.addonics.com/support/ticketid/create.asp or phone USA 408-453-6212
Copyright © 2011 Addonics Technologies, All rights reserved.

Choosing Automatic will configure the Secure NAS unit as a DHCP client and the configuration wizard will skip to the end. Choosing Manual configuration will proceed to Step 2.

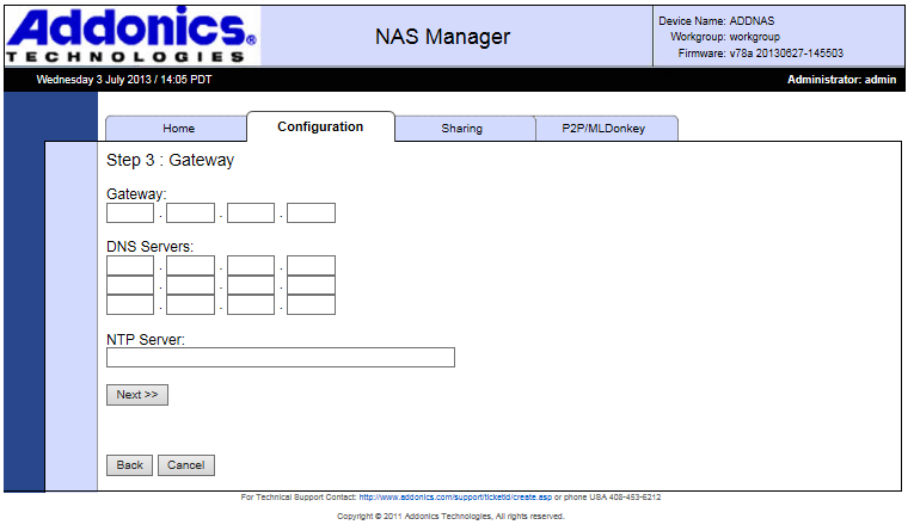


Step 2 configures the Secure NAS unit's static IP address and subnet mask. To choose a working static IP address, make sure you meet these criteria:

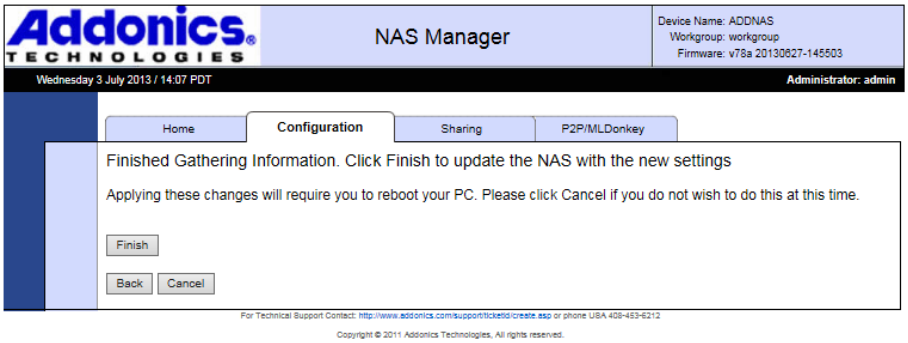
1. The subnet mask must match the rest of the network exactly.
2. The IP address must match the router's IP address exactly where the subnet mask is "255."
3. The IP address cannot end in 0 or 255.
4. The IP address must not match any other system on the network.
5. The IP address should not be within the DHCP server's client pool.



The next step is to configure network connections. The gateway is usually the internal IP address for the router the Secure NAS unit is connected to. DNS entries are usually the same as used by the router's external network configuration (determined by your ISP). Setting an NTP server will synchronize the Secure NAS unit to a time server, usually on the Internet. This can be a name or IP address. Use the keywords “free NTP servers” on your preferred search engine if you wish to configure this feature and don't know of a server you can use.

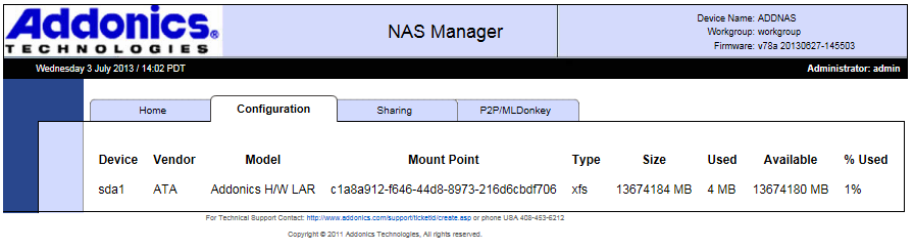


When the wizard is complete by either choosing Automatic in Step 1 or completing Steps 2 and 3, a confirmation page will appear. Clicking the Finish button will apply the settings.


Addonics TECHNOLOGIES
NAS Manager
Device Name: ADDNAS
Workgroup: workgroup
Firmware: v78a 20130627-145503
Wednesday 3 July 2013 / 14:07 PDT
Administrator: admin
Home
Configuration
Sharing
P2P/MLDonkey
Finished Gathering Information. Click Finish to update the NAS with the new settings
Applying these changes will require you to reboot your PC. Please click Cancel if you do not wish to do this at this time.
Finish
Back
Cancel
For Technical Support Contact: http://www.addonics.com/support/ticketid/create.asp or phone USA 408-453-6212
Copyright © 2011 Addonics Technologies, All rights reserved.

View Drive Information
Displays details of all connected drives. If network shares are configured for drives that have been disconnected, those drives will also appear in this list as unavailable.

Device: The letter after “sd” is the drive's letter, in order of when the drive was first encountered by the NAS unit. The number at the end of the device label is the partition on the drive, in order of the drive's partition map.
Vendor: The drive's manufacturer.
Model: The drive's model number.
Mount Point: Used by the Secure NAS unit internally.
Type: The file system the partition is formatted with.
Size: The total space of the partition.
Used: Space in use on the partition.
Available: Remaining space available on the partition.
% Used: Percentage of the partition space in use.


Addonics TECHNOLOGIES
NAS Manager
Device Name: ADDNAS
Workgroup: workgroup
Firmware: v78a 20130627-145503
Wednesday 3 July 2013 / 14:02 PDT
Administrator: admin
Home
Configuration
Sharing
P2P/MLDonkey
Device Vendor Model Mount Point Type Size Used Available % Used
sda1 ATA Addonics H/W LAR c1a8a912-f646-44d8-8973-216d6cbdf706 xfs 13674184 MB 4 MB 13674180 MB 1%
For Technical Support Contact: http://www.addonics.com/support/ticketdisplay.asp or phone USA 408-453-6212
Copyright © 2011 Addonics Technologies, All rights reserved.

View User Samba and FTP Login Information

Displays a list of open sessions for file sharing of Windows sharing and FTP. The login username, the computer's hostname and IP address are listed for each session.

Format Drive
Formats a specific drive using a choice of ext3 or XFS file systems.
Caution: this function destroys data.

Choose a drive to format. If the drive is greater than 2TB in capacity choose the GPT boot record, otherwise choose MBR. Finally, choose Linux EXT3 or Linux XFS for the file system. After clicking Format Drive, the format utility will request confirmation.

NOTE: For highest possible performance, use the XFS file system.

After clicking “Yes, I'm sure,” the format utility will create and prepare one partition on the selected drive, using all space on the disk. A page will load next confirming the format is in progress. This page updates once every minute. Once formatting is complete, the page will change to state it is done. Click any of the tabs above the message to perform other tasks. If desired, this can be done before formatting is complete; however, the drive being formatted cannot be used until formatting is done and there will be no further notifications.

Safely Remove Drive

Closes all pending I/O to a specified drive then “unmounts” it for removal.
Caution: best practice is to notify any and all users this will be done before proceeding to prevent data loss. Abruptly removing a physical drive without notifying users or using the Safely Remove Drive function may cause file system corruption and loss of data.

Backup Internal System Configuration Information

Saves or restores all of the Secure NAS unit's settings using a specified drive. Select the volume desired for backups. If backups exist on that volume they will be listed under Backups, with comments if present.
To create a backup, add a backup comment if desired then click Create Backup. To restore an existing backup, select the desired backup and click Restore Selected. The currently selected backup may also be deleted using the Delete Selected button. All three functions will request confirmation before proceeding.

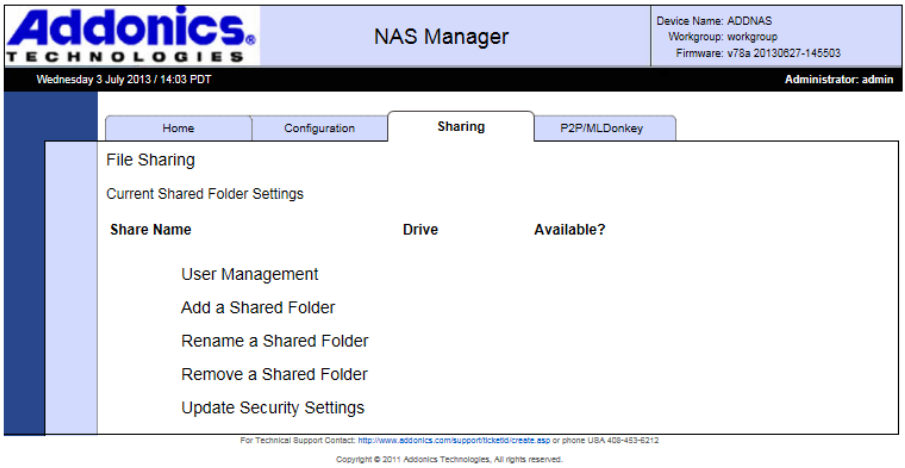
Reboot

Restarts the Secure NAS unit.
Caution: best practice is to notify any and all users this will be done before proceeding

Upgrade the System Firmware
In the case of a firmware update release, this utility applies the update. Update will not proceed unless only one volume (one partition on one drive) is present. Instructions on updating firmware are provided with the firmware update.

Caution: All of the Secure NAS unit's settings will be lost in the process of applying firmware. Make sure to notify any and all users this will be done to prevent data loss and use the Backup Internal System Configuration Information utility before proceeding.

The Sharing Tab



User Management

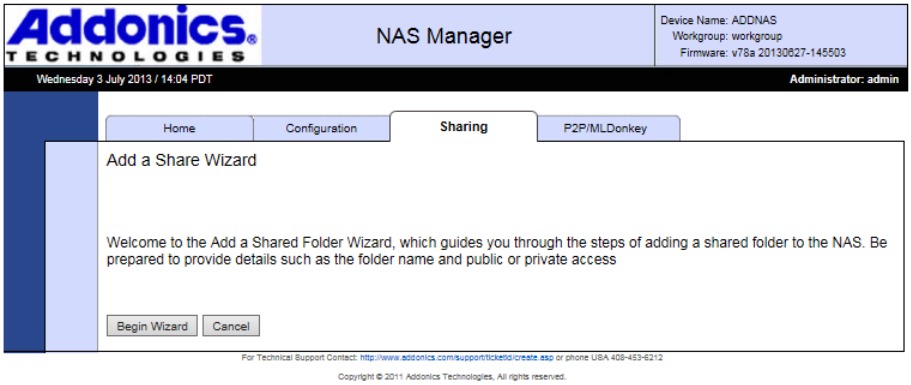
Shows current list of known users on the Secure NAS unit.

To delete a user, click the “Delete” link next to that username, then confirm.
To change a user's password, select the username just above “New Password,” then enter the new password into the “New Password” and “Confirm Password” fields and click “Change Password.”

To create a new user account, click “New User,” then enter the new username and the initial password in the “New Password” and “Confirm Password” fields. If shared folders are defined on the system, select the default permissions granted to the new user for each share.

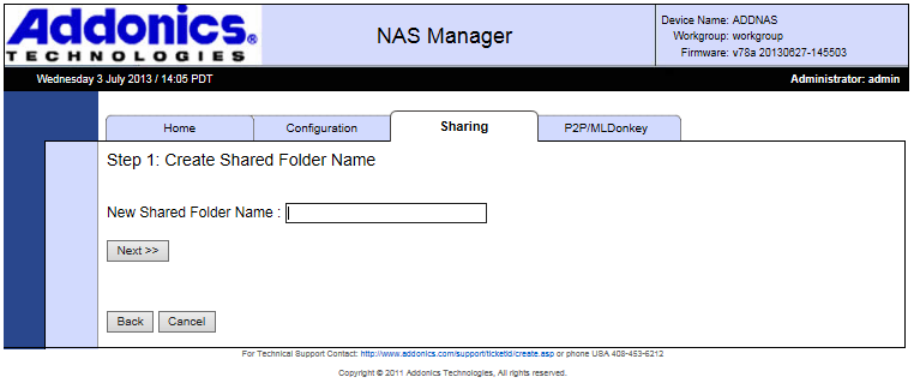
Add A Shared Folder

Creates a new folder and shares it on the network. This function has several steps. The first page introduces the wizard. Click “Begin Wizard” to proceed.

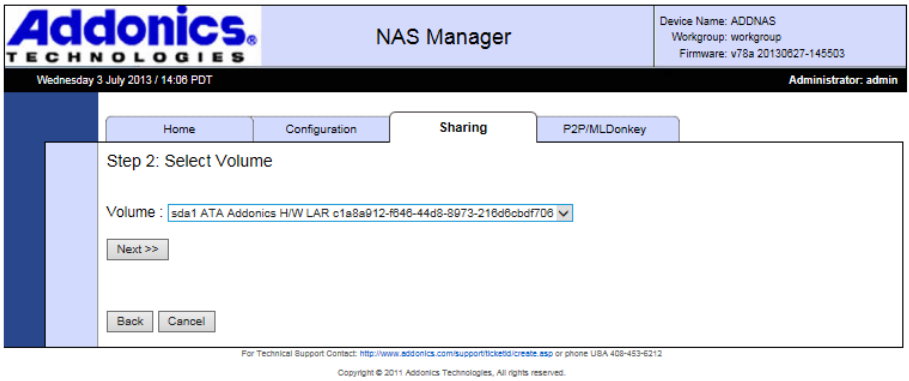

Addonics TECHNOLOGIES
NAS Manager
Device Name: ADDNAS
Workgroup: workgroup
Firmware: v78a 20130627-145503
Wednesday 3 July 2013 / 14:04 PDT
Administrator: admin
Home
Configuration
Sharing
P2P/MLDonkey
Add a Share Wizard
Welcome to the Add a Shared Folder Wizard, which guides you through the steps of adding a shared folder to the NAS. Be prepared to provide details such as the folder name and public or private access
Begin Wizard
Cancel
For Technical Support Contact: http://www.addonics.com/support/ticketdi/create.asp or phone USA 408-453-6212
Copyright © 2011 Addonics Technologies, All rights reserved.

Step 1 is to define the name of the share. The share name will become the folder name on the drive.

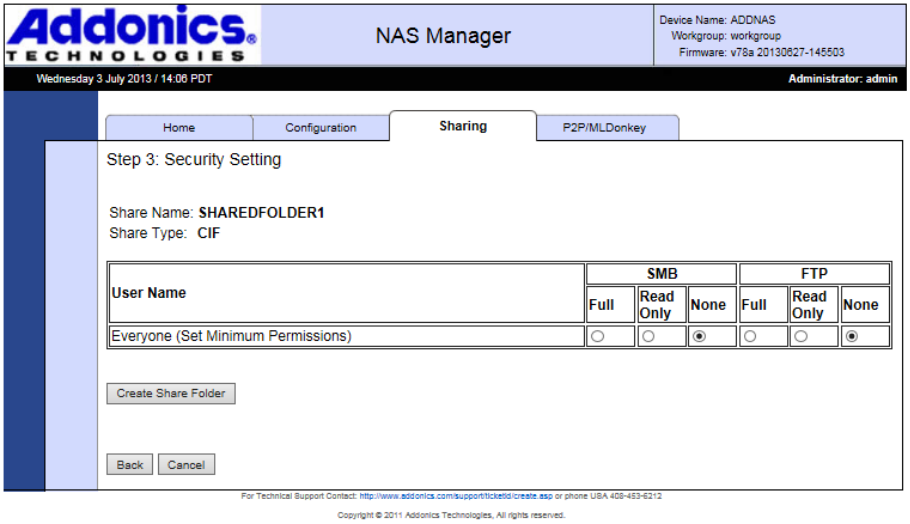
NOTE: The shared folder name will be written to disk using all capital letters. If an existing folder of the same name appears and is not all capital letters, the Secure NAS considers that not a match and writes the same folder name in all capital letters anyway. This can cause unpredictable results if the drive is subsequently connected to a computer. If a folder exists of the same name with all capital letters, it will be shared without harming any data.



Step 2 is to select the drive the share is to be created on. The drive is identified by the drive letter and partition number, the vendor and model, and the mount point.



Step 3 is to set the initial permissions for the new share. A permission setting for "Everyone" as well as each individual user is listed, with the default permission set to None for both SMB and FTP. Once you have reviewed the permissions for all users and made any desired changes, clicking on "Create Share Folder" will complete the Wizard.



Rename A Shared Folder

Changes the name of the directory as well as the share name for an existing shared folder. Select the share to change and type in a new name, then click "Rename Shared Folder."

NOTE: The new shared folder name will be written to disk using all capital letters. If an existing folder of the same name appears and is not all capital letters, the Secure NAS considers that not a match and writes the same folder name in all capital letters anyway. This can cause unpredictable results if the drive is subsequently connected to a computer. If a folder exists of the same name with all capital letters, it will be shared without harming any data.

Remove a Shared Folder

Deletes a share from the Secure NAS unit. As a precaution this screen requires the word “yes” is typed in as confirmation.
NOTE: Removing a shared folder also deletes the associated directory and all of its contents from the drive. It is however possible to delete the share without destroying any data: simply disconnect the drive physically from the Secure NAS unit before proceeding. If the shared folder is on the Secure NAS unit's RAID array, shutting down the unit, then removing all of the RAID drives and powering up again before deleting the share will preserve the data.

Update Security Settings

Changes SMB and FTP permissions for a share for each user and the general permission for “Everyone.” Select the share to change, then click next and another page will appear with current permissions. Make desired changes and click Update to apply.

CONTACT US

www.addonics.com
Phone: 408-573-8580
Fax: 408-573-8588
Email: http://www.addonics.com/sales/query/